Applied Algebra, MAT312/AMS351
Practice Problems for Midterm 1: Solutions

1. Find the greatest common divisor of $12n + 1$ and $30n + 2$.
Solution: $30n + 2 = 2(12n + 1) + 6n$; $12n + 1 = 6n \cdot 2 + 1$. Thus $\gcd(12n + 1, 30n + 2) = 1$.

2. Prove that for every natural number n, the number $3^{2n+2} + 8n - 9$ is divisible by 16.
Solution: Induction on n.
Base: $n = 0$, $3^{2n+2} + 8n - 9 = 0$.
Step: we assume that $3^{2k+2} + 8k - 9$ is divisible by 16. For $n = k + 1$, the expression becomes $3^{2(k+1)+2} + 8(k + 1) - 9 = 9(3^{2k+2} + 8k - 9) - 64k + 80$.
Since $3^{2k+2} + 8k - 9$, $64k$, and 80 are divisible by 16, so is $3^{2(k+1)+2} + 8(k+1) - 9$.

3. Recall that the Fibonacci sequence is defined as $F_1 = 1, F_2 = 1$, and then for every $n > 2$, $F_n = F_{n-1} + F_{n-2}$. Prove that for every n, $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.
Solution: Induction on n.
Base: $n = 1$. $F_1 = F_2$ (both equal 1.
Step: we assume that $F_1 + F_3 + \cdots + F_{2k-1} = F_{2k}$. Then $F_1 + F_3 + \cdots + F_{2(k+1)-1} = (F_1 + F_3 + \cdots + F_{2k-1}) + F_{2(k+1)-1} = F_{2k} + F_{2k+1} = F_{2k+2} = F_{2(k+1}$.

4. Find all $n > 2$ such that $n^3 - 3$ is divisible by $n - 1$.
Solution: $n^3 - 3 = (n - 1)(n^2 + n + 1) - 2$. If $n^3 - 3$ is divisible by $n - 1$, $n - 1$ divides 2, i.e. $n - 1 = 1, 2$. Given that $n > 2$, we conclude that $n = 3$.

5. When questioned by the police, the suspect claimed that he did not remember his home address but could definitely recall that the house number is less than 1000 and is divisible by 7, 11, and 13. Is the suspect telling the truth?
And what if he said that the number was divisible by 7, 11, and 14?
Solution: Since 7, 11, and 13 are relatively prime, a number divisible by them must be divisible by their product. (This follows from the Unique Factorisation Theorem.) But $7 \cdot 11 \cdot 13 = 1001$, so the house number is both less than 1000 and divisible by 1001.
However, if a number is divisible by 7, 11, and $14 = 2 \cdot 7$, it should only be divisible by $2 \cdot 7 \cdot 11 = 154$, i.e. may be less than 1000.

6. Let a, b, and c be positive integers such that $a^2 + b^2 = c^2$. Prove that at least one of them is divisible by 3.
Solution: Reducing mod 3, we get $[a]_3^2 + [b]_3^2 = [c]_3^2$. If neither a, b nor c are divisible by 3, then they belong to either $[1]_3$ or $[-1]_3$. Hence $[a]_3^2 = [b]_3^2 = [c]_3^2 = [1]_3$ and the equality does not hold.

7. Solve the following linear congruences:
(a) $5x \equiv 7 \mod 31$;
Solution: $\gcd(5, 31) = 1$, hence the solution is $[5]_{31}^{-1}[7]_{31}$. To compute $[5]_{31}^{-1}$, we first perform the Euclidean algorithm for the pair $(5, 31)$: $31 = 5 \cdot 6 + 1$. Therefore $31 + 5(-6) = 1$, i.e. $[5]_{31}^{-1} = [-6]_{31}$. Finally, $[5]_{31}^{-1}[7]_{31} = [-6]_{31}[7]_{31} = [-42]_{31} = [20]_{31}$.

(b) $2x \equiv 19 \mod 2006$;
Solution: $\gcd(2, 2006) = 2$ does not divide 19. No solutions.

(c) $19x + 3 \equiv 4 \mod 83$.
Solution: If $19x + 3 \equiv 4$, then $19x \equiv 1$. Thus $x = [19]_{83}^{-1}$. Euclidean algorithm for 19 and 83: $83 = 19 \cdot 4 + 7$; $19 = 7 \cdot 2 + 5$; $7 = 5 \cdot 1 + 2$; $5 = 2 \cdot 2 + 1$. Then $2 \cdot 2 = 5 - 1$; $7 \cdot 2 = 5 \cdot 2 + 2 \cdot 2 = 5 \cdot 3 - 1$; $19 \cdot 3 = 7 \cdot 2 \cdot 3 + 5 \cdot 3 = 7 \cdot 6 + 7 \cdot 2 + 1 = 7 \cdot 8 + 1$; $83 \cdot 8 = 19 \cdot 4 \cdot 8 + 7 \cdot 8 = 19 \cdot 32 + 19 \cdot 3 - 1 = 19 \cdot 35 - 1$. Hence, $19 \cdot 35 \equiv 1 \mod 83$. (Alternatively, you could use the matrix method.) Answer: $[35]_{83}$.

8. Find the minimal positive integer satisfying the following conditions:
(i) when divided by 7, its remainder is 4,
(ii) when divided by 12, its remainder is 5.
Solution: We have to find x such that

$$\begin{cases} x \equiv 4 \mod 7 \\ x \equiv 5 \mod 12. \end{cases}$$

Since $7 \cdot (-5) + 12 \cdot 3 = 1$, by the Chinese Remainder Theorem, the solution is $[5 \cdot 7 \cdot (-5) + 4 \cdot 12 \cdot 3]_{7 \cdot 12} = [-31]_{84} = [53]_{84}$. Answer: 53.

9. Compute $\phi(1001)$, $\phi(96)$.
Solution: $1001 = 7 \cdot 11 \cdot 13$, thus $\phi(1001) = \phi(7)\phi(11)\phi(13) = 6 \cdot 10 \cdot 12 = 720$. $96 = 2^5 \cdot 3$, thus $\phi(96) = \phi(2^5)\phi(3) = (2^5 - 2^4) \cdot 2 = 32$.

10. Find the last two digits of 1221^{122}.
Solution: Last two digits of any number = remainder of division by 100. Therefore, we have to compute $[1221^{122}]_{100}$. Simplifying, $[1221^{122}]_{100} = [1221]_{100}^{122} = [21]_{100}^{122}$. By Euler's theorem $[a]_{100}^{\phi(100)} = [1]_{100}$. Since $\phi(100) = \phi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 40$, $[21]_{100}^{122} = [21]_{100}^{2} = [441]_{100} = [41]_{100}$. Answer: 41.